Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Organizational Requirements - Policies, Procedures, and Documentation Requirements

Audit Objective:

1. Ensure that security policies and procedures have been developed and promulgated appropriately throughout the organization. (Estimated Hours = 17)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
1.1.	Identify a retention policy and/or procedures for the organization's security policies and procedures.			
1.2.	Verify that the security policies carry effective dates. Look for a change history associated with each policy and carrying dates of changes. Ensure that the date when a policy became inactive is clearly documented or easily inferred.			
1.3.	Verify that all workforce members are able to access the policies and other security documents they need. This may occur through a combination of electronic and paper copies.			
1.4.	Ensure that the responsibility for periodic (usually annual) review of security policies has been designated to a person or position in the organization.			
1.5.	Verify that security policies and procedures are reviewed on a standard timeframe.			
1.6.	Verify that there is a procedure for policy updates and creation of new policies.			
1.7.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards - Security Management Process Standard - Policy-Making Process

Audit Objective:

2. Ensure that the organization has a formal (i.e., written) process for information security policy development, review, approval, and dissemination. (Estimated Hours = 15)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
2.1.	Identify a written policy and procedures for policy development, modification, and obsolescence.			
2.2.	For information security, ensure that the procedures identify who may initiate or propose a policy or modification, and how.			
2.3.	Ensure that the procedures identify what body (for example, the Information Security and Privacy Committee or the Organization's Management Team) is responsible for review and acceptance of an information security policy.			
2.4.	Ensure that the procedures identify who signs the policy after review and acceptance by the designated committee, making it official and, thus, enforceable (for example, the CEO or Agency Director).			
2.5.	Ensure that the procedures identify how policies are named/numbered and where they are stored. (This is an important repository and its location should be appropriately secure).			
2.6.	Ensure that the procedures describe how the workforce is made aware of the new policy and its implications. (For example, an email blast is sent describing the policy and carrying a link to the document. The key points are incorporated in the workforce security training curriculum.)			
2.7.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards - Security Management Process Standard - Risk Analysis/Risk Management

Audit Objective:

3. Ensure that the organization has conducted a thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of Protected Health Information (PHI), and ensure that the organization has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. (Estimated Hours = 16)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
3.1.	Identify the organization's policy commitment to performing risk assessment.			
3.2.	Obtain a written report documenting the risk assessment.			
3.3.	Verify that the risk assessment covers the full scope of administrative, physical, and technical risks and vulnerabilities to PHI.			
3.4.	Verify that the risk assessment identifies risks and assigns a priority of weight to each.			
3.5.	Verify that there are action plans for mitigating each significant risk.			
3.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards - Security Management Process Standard - Sanction Policy

Audit Objective:

4. Ensure that the organization has a sanction policy and guidelines for handling privacy and security violations or breaches. (Estimated Hours = 21)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
4.1.	Determine if there are privacy and security violation/breach sanction policies or an equivalent policy statement contained within a related policy.			
4.2.	Ensure that the policies explicitly apply to the full workforce.			
4.3.	Identify sanctions procedures and guidelines that consider intent, pattern of behavior, and severity of impact (or potential impact).			
4.4.	Review documentation of security incidents and sanctions to verify that sanctions follow guidelines; that they consider intent, pattern of behavior, and impact; and that they appear consistent.			
4.5.	Verify that privacy and security incidents are documented in separate security incidents and privacy incidents databases [Note: The majority of privacy breaches are also security (confidentiality) breaches; however, not all security breaches are privacy breaches.]			
4.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards - Security Management Process Standard – Information System Activity Review

Audit Objective:

5. Ensure that the organization has implemented procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. (Estimated Hours = 13)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
5.1.	Identify sources of system activity used for security review.			
5.2.	Verify that sources include some level of audit logs (e.g., OS, database, patient record access in application) and security incident reports. (Note that this may vary widely in different environments).			
5.3.	Verify that procedures identify responsible parties.			
5.4.	Verify that procedures identify frequency of review of each type of activity.			
5.5.	Verify that the procedures describe or give guidance on what to look for (what activity may indicate a breach) and how to respond.			
5.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards - Assigned Security Responsibility Standard

Audit Objective:

6. Ensure that the organization has identified the security official who is responsible for the development and implementation of the security policies and procedures. Generally, this position is referred to as the Information Security Officer (ISO). (Estimated Hours = 13)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
6.1.	Ensure that the ISO is identified in an official written document.			
6.2.	Ensure that the workforce knows who the ISO is and how to contact the ISO about information security matters. (This is typically included in workforce training.)			
6.3.	Verify that the ISO job description is documented.			
6.4.	Ensure that the ISO job description identifies the ISO as the point of contact for security policy, implementation, and monitoring.			
6.5.	Verify that the ISO oversees the development and communication of security policies and procedures.			
6.6.	Ensure that the ISO has documented reporting giving him/her adequate visibility and authority to carry out his/her role.			
6.7.	Verify that the ISO is placed within the organizational hierarchy with the shortest practicable reporting lines to the CEO or Agency Director.			
6.8.	Ensure that job descriptions for IT staff and managers, who authorize access, include an explanation of their security role and responsibilities.			
6.9.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards - Workforce Security Standard - Authorization and/or Supervision

Audit Objective:

7. Ensure that all members of the organization's workforce have appropriate access to electronic PHI. (Estimated Hours = 10)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
7.1.	Verify that people using computers are authorized (e.g., have their own unique userID).			
7.2.	Verify that there is a policy and/or procedures stating that workforce members not authorized to access PHI must be supervised in areas where PHI is exposed.			
7.3.	Verify through observation that unauthorized workforce members (and others such as copier repair service workers) are in fact supervised when in areas where PHI, in any form, is exposed.			
7.4.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards - Workforce Security Standard - Workforce Clearance Procedure

Audit Objective:

8. Ensure that procedures have been implemented by the organization to determine that the access of a workforce member to electronic Protected Health Information (PHI) is appropriate. (Estimated Hours = 8)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
8.1.	Verify that human resources' documented procedures include performing adequate background checks on new employees, and, perhaps on employees changing positions. This is important for all workforce members since some incidental disclosures of PHI are likely to occur, but it is particularly important when the person will be granted access to PHI.			
8.2.	Verify that comparable, documented clearance procedures exist and are followed for non-employee members of the workforce, or at least those who will be granted access to PHI. These procedures are likely to vary widely, depending on the type of non-employee workforce member (e.g., student vs. volunteer).			
8.3.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards - Workforce Security Standard - Termination Procedures

Audit Objective:

9. Ensure that the organization has implemented procedures for terminating access to Protected Health Information (PHI). (Estimated Hours = 15)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
9.1.	Ensure that written termination procedures are clear and comprehensive regarding de-activation of electronic access.			
9.2.	Verify that termination procedures exist for employees as well as for every other type of workforce or third party who may have access to the organization's PHI.			
9.3.	Verify that the notification procedures reach every point of user access that is to be de-activated.			
9.4.	Verify that the termination procedures have a defined timeframe for the de-activation and subsequent notification to the organization.			
9.5.	Verify that there are special procedures for immediate termination of access. Procedures should identify circumstances requiring or suggesting immediate termination, who is authorized to invoke immediate termination of access, contact information, and timing considerations.			
9.6.	Ensure that there are explicit instructions for every one of the organizations system on how to de-activate a user account.			
9.7.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Information Access Management Standard – Access Authorization

Audit Objective:

10. Ensure that the organization has policies and procedures for granting access to electronic Protected Health Information (PHI). (Estimated Hours = 8)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
10.1.	Verify that an organization policy (or procedure in a small organization) requires that an individual's access to PHI must be authorized by an appropriate manager (or position of authority), must be required for the person's job, and must be at the minimum necessary level.			
10.2.	Obtain documentation specifying who has the authority to authorize access to PHI. This may be one individual (in a small office), a list of individuals, or it may be a list of roles.			
10.3.	Verify that the individual's access authorization is documented on a form (paper or electronic).			
10.4.	Ensure that the authorization procedures require that the authorizer specify the access privileges to be assigned to each individual (or role, if the organization uses role-based access control). The access privileges need to span all the various levels of access and systems of the organization that contain PHI.			
10.5.	Verify that access procedures also cover notification of a change to a user's access privileges. The same policy should apply: it must be authorized, needed for the job, and be at a minimum necessary level.			
10.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Information Access Management Standard – Access Establishment and Modification

Audit Objective:

11. Ensure that the organization has policies and procedures which establish, document, review and modify a user's right of access to a workstation, transaction, program or process. (Estimated Hours = 8)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
11.1.	Ensure that access procedures indicate how the security administrator, or person setting up users, is expected to review the form for completeness and appropriateness.			
11.2.	Ensure that there are written, detailed instructions for the security administrator to follow, upon receipt of a form, in setting up a user account and assigning and modifying access privileges.			
11.3.	Ensure that there are instructions for the security administrator to follow in completing the form and filing it. Usually the administrator signs and dates the form, and then files it where it can be retrieved if necessary.			
11.4.	Ensure that there are instructions for the security administrator on how to securely convey the user ID and password (or other means of authentication) to new users.			
11.5.	Verify that there are procedures for periodic reporting of users with access to PHI, and a review of those users and their access privileges. This is a standard safety net for catching overlooked terminations and job changes).			
11.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Security Awareness and Training Standard

Audit Objective:

12. Ensure that the organization has implemented a security awareness and training program for all members of its workforce, including management. (Estimated Hours = 7)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
12.1.	Ensure that the workforce security training reaches the entire workforce (including full-time, part time, classified, hourly, temporary agency employees, contract employees, students, interns, and volunteers), and management. The mandatory training requirement should be defined as a policy-level commitment.			
12.2.	Ensure that workforce training is given with sufficient frequency (e.g. annually) to reinforce the message and indicate that security is important to the organization. Training should also be provided whenever there are changes affecting security. There should be a policy statement or other written document to ensure this commitment.			
12.3.	Ensure that workforce training materials are always available to the workforce, and that workforce members know how to obtain access and/or copies. Materials may be on an intranet (but provide alternatives for individuals without network access), and there may be hard-copy handouts. If training is online, ensure that users can print training materials on demand.			
12.4.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Security Awareness and Training Standard – Security Reminders

Audit Objective:

13. Ensure that the organization has implemented procedures to perform periodic security reminders to the entire workforce. (Estimated Hours = 4)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
13.1.	Verify that periodic reminders have been delivered to the workforce (Someone should be keeping a file of documentation showing that reminders have been issued.) These reminders should be reaching the organizations full workforce.			
13.2.	Verify that there is a documented plan for ongoing periodic reminders including a reasonable schedule (e.g, monthly) and a person responsible for delivering them.			
13.3.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Security Awareness and Training Standard – Protection from Malicious Software

Audit Objective:

14. Ensure that the organization performs workforce training to guard against, detect, and report malicious software such as computer viruses and worms. (Estimated Hours = 10)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
14.1.	Verify that standard workforce security training materials include reference to malware: how to avoid malware, signs of malware, and how to report suspected malware.			
14.2.	Verify if the organization pushes anti-virus software to the user's workstation or if the organization reminds the users pull anti-virus software updates to their workstations. If the organization requires the users to update their anti-virus signature file, determine if there are clear instructions on how and how often the users are supposed to perform the updates.			
14.3.	Ensure that the appropriate technical mechanisms are in place to catch and stop the spread of malware on the organization's network. The locations of where the protection software is installed, how often it is updated, and how users' workstation – fixed and portable – should be considered.			
14.4.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Security Awareness and Training Standard – Log-In Monitoring

Audit Objective:

15. Ensure that procedures are in place to monitor workforce log-in attempts, in conjunction with workforce training on how to report login discrepancies. (Estimated Hours = 3)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
15.1.	Determine if the organization systems provide a last-logon message, and if the system security policies remind users to read and report discrepancies. If this security feature is included in the policy, ensure that it is documented in the workforce training materials.			
15.2.	Ensure that training materials include a reminder to report any significant change or sudden and persistent slow-down on user workstations.			
15.3.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Security Awareness and Training Standard – Password Management

Audit Objective:

16. Ensure that the organization has implemented procedures for creating, changing and safeguarding of passwords. (Estimated Hours = 6)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
16.1.	Ensure that workforce training includes instructions on how to make up good passwords (e.g., a mix of numbers and letters) and what not to do (e.g., no real words, imaginary characters' names, number strings such as birth date etc…). Good passwords should be easy for the user to remember but hard for someone else to guess.			
16.2.	Ensure that workforce training prohibits sharing passwords with anyone else (even IT), writing passwords down where they can be found, putting them in a logon script, or selecting "save my password" when that is an option.			
16.3.	Determine if the organization's systems support the feature of changing a password at will (e.g., when a user suspects someone else knows his/her password). If this technical feature is supported, ensure that the workforce is given written (paper or electronic) instructions on the procedure.			
16.4.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Security Incident Procedures Standard – Response and Reporting

Audit Objective:

17. Ensure that the organization has implemented policies and procedures to identify and respond to suspected or known security incidents. (Estimated Hours = 6)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
17.1.	Ensure that security policy or procedures define security incidents broadly and give examples to make this point clear to the organization. Ensure that training also includes definitions and examples security incidents.			
17.2.	Ensure that reporting procedures are in place for both technical incidents (usually identified in the IT department) and non-technical incidents (can be reported by any workforce member). Determine if the organizations has an incident reporting form to capture all relevant information about the incident as well as a corrective steps subsequently taken.			
17.3.	Ensure that there is a clear response plan for a variety of incidents. Usually organizations proactively identify a variety of the most likely incidents and develop response guidelines for each.			
17.4.	Ensure that a response team (or responsibly individual such as the ISO) is identified and that members' role are identified. (For example, who will make the decision to notify law enforcement?) Often there is a core team led by the ISO, with a second tier team who are called on as needed. (For example, a human resource representative would be involved with an employee incident, but probably not with a network intrusion incident).			
17.5.	Ensure that steps take to mitigate any harmful effects are documented.			
17.6.	Ensure that incident reports are analyzed to determine if the organization should make technical, policy, training, or other changes to reduce the risk of a repeat. Any such security changes should be documented with the incident reporting logs.			
17.7.	Determine if the organization has a security policy which states that it will respond, document and mediate any security breach.			
17.8.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Contingency Plan Standard – Data Backup Plan

Audit Objective:

18. Ensure that procedures have been implemented to create and retrieve exact copies of electronic Protected Health Information (PHI). (Estimated Hours = 14)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
18.1.	Ensure that backup procedures identify each file to be backed up, how often, through what utility (with run instructions) and onto what medium.			
18.2.	Ensure that backup procedures specify how long each backup file is to be kept.			
18.3.	Ensure that backup procedures specify where the offsite copies are kept, how they are transported there safely, and how they can be retrieved – both under normal circumstances and in an emergency.			
18.4.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Contingency Plan Standard – Disaster Recovery Plan

Audit Objective:

19. Ensure that the organization has implemented procedures to restore any loss of data resulting from any natural, environmental and man-made disasters. (Estimated Hours = 11)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
19.1.	Verify that recovery procedures identify roles and responsibilities of those identified in the disaster recovery plan (DRP), including any third party contacts.			
19.2.	Verify that recovery procedures include current contact information for all relevant parties including staff and vendors. Determine if contact information is required and valid for 24 x 7 or just during regular business hours.			
19.3.	Verify that recovery procedures include explicit run instructions (codes) and configuration options. (Often the documentation refers to these executables stored on compact disc as part of the disaster recovery plan.)			
19.4.	Determine that if alternate sites (hot sites) are required in the DRP, and whether the alternate site contracts, agreements and logistics details are clearly documented.			
19.5.	Verify that an up-to-date copy of the DRP is kept securely (and readily available) both on-site and off-site.			
19.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Contingency Plan Standard – Emergency Mode Operation Plan

Audit Objective:

20. Ensure that procedures have been implemented that enable the continuation of critical business processes and providing for the security of Protected Health Information (PHI), when the organization is operating in emergency mode. (Estimated Hours = 6)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
20.1.	Verify that there is a security procedure for protecting PHI if and when there is heightened risk of a crisis. One procedure example would be to physically guarding an area with portable media containing PHI, should electronic doors not be functioning.			
20.2.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Contingency Plan Standard – Testing And Revision Procedure

Audit Objective:

21. Ensure that the organization has implemented procedures for the periodic testing and revision of contingency plans, including both partial and alternative testing. (Estimated Hours = 12)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
21.1.	Ensure that there are procedures for periodic testing of contingency plans. Procedure should specify who is responsible, how to conduct the testing, and how often the testing is done.			
21.2.	Ensure that the testing procedures require that deficient plan contents be updated within a reasonable time frame. (It is also recommended that these procedures require review and sign-off on all plan updates by the disaster recovery team or the organization's management team).			
21.3.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Contingency Plan Standard – Applications and Data Criticality Analysis

Audit Objective:

22. Ensure that the organization has performed a criticality assessment of its applications and data, in order to support the components of the contingency plan. (Estimated Hours = 14)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
22.1.	Ensure that there is an inventory of applications and data including all electronic PHI.			
22.2.	Verify that there is documentation of the criticality analysis process including the methodology uses. This criticality analysis could include, but not be limited to, include team members, detailed procedures, a work plan and forms.			
22.3.	Verify that the procedures resulted in a relative criticality rating for each application and set of data, including those applications and data identified as high priority requiring appropriate prioritization of support and recovery activities.			
22.4.	Verify that the critical applications and data are covered by the disaster recovery plan (DRP).			
22.5.	Ensure that these or other procedures require adding new applications or data to the inventory, rating the criticality of any new applications or data, and, if appropriate, preparing a revised DRP.			
22.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Evaluation Standard

Audit Objective:

23. Ensure that the organization performs periodic technical and non-technical evaluations that establish that the organizations policies and procedures meet the compliance requirements of appropriate security for its Protected Health Information (PHI). Ensure that subsequent compliance evaluations are performed on privacy and security policies and procedures when there is an operational or environment change to the organization's security of PHI. (Estimated Hours = 13)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
23.1.	Ensure that a compliance audit has been performed and documented.			
23.2.	Ensure that any standards or specifications not adequately met at the time of the audit have been identified.			
23.3.	Ensure that any deficiencies identified in the compliance audit have been addressed. (It is suggested that organizations have the person performing the original audit return to review new documentary evidence of compliance.)			
23.4.	Ensure that policy and/or procedure require future re-evaluation in response to environmental or operational changes affecting the security of PHI. Determine if the organization's procedures include compliance audits performed on a periodic basis (e.g. bi-annually).			
23.5.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Administrative Safeguards – Business Associate Contracts and Other Arrangement Standard
Organizational Requirements - Business Associate Contracts or Other Arrangements Standard

Audit Objective:

24. Ensure that written contracts or other permitted arrangements exist with all of the organization's business associates. The business associate contracts must include mandated contracting language to protect the confidentiality, integrity and availability of the organization's Protected Health Information (PHI) when created, accessed, used or disclosed by the business associate. (Estimated Hours = 12)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
24.1.	Ensure that the privacy Business Associate Contract (BAC), Business Associate Agreement (BAA, Memorandum of Understanding – MOU) or any other arrangement has been amended to include the following points explicitly required: "The contract between covered entity and business associate must provide that the business associate will – (A) Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic protected health information (PHI) that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract."			
24.2.	Determine for each of the organizations business associates (BA), including those which are governmental agencies, that a signed amended (HIPAA-mandated) contract, agreement or MOU exists. If statutory obligations exist outside of HIPAA requirements, the cited laws or statutory obligations should be documented.			
24.3.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Physical Safeguards – Facility Access Controls Standard – Contingency Operations

Audit Objective:

25. Ensure that the organization has procedures documented under the disaster recovery and emergency mode operations plans to allow physical access to its electronic information systems and facilities in order to recover lost data resulting from an emergency event. (Estimated Hours = 18)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
25.1.	Ensure that contingency access plans or procedures are documented.			
25.2.	Ensure that contingency access plans are appropriate to the organizations disaster recovery plan.			
25.3.	Ensure that contingency access plans are adequate to protect PHI. The plans will allow facility access in support of restoration of lost data in the event of an emergency.			
25.4.	Ensure that adequate preventive maintenance is performed on mechanical equipment and air conditioning.			
25.5.	Perform a walk-through of the data center and surrounding areas and determine through observation if: a) A UPS is used to supplement and backup the normal electrical power system. b) The alternative power source is located in a secure location. c) The computer center has its own separate incoming power supply and circuit control box. d) Circuit control boxes are locked and located in a secure location. e) Circuit breaker panels are marked to expeditiously reference equipment. f) There are adequate air conditioner units to provide backup. Computer center air conditioners are separate from building air conditioner systems.			
25.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Physical Safeguards – Facility Access Controls Standard – Facility Security Plan

Audit Objective:

26. Ensure that the organization has implemented policies and procedures to safeguard its facility and equipment from unauthorized physical access, tampering and theft. (Estimated Hours = 11)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
26.1.	Verify that there is a facility security plan identifying what physical and procedural security controls are in place. Ensure that it covers all doors, stairs and elevator entry points.			
26.2.	Verify that the plan includes locks for external and internal entryways (for example, data center and server closet) as needed: where located, when they are locked/unlocked, and the system for how they are operated (e.g., keys, access cards, proximity badge, etc…)			
26.3.	Verify that the plan for locks includes identification of who controls access and other details. If keys are used, ensure there is documentation of who has master keys (minimum necessary). If keypad locks, ensure there is documentation for when and how codes are changed and protected. If access or proximity cards, ensure there is documentation on who administers the system and how.			
26.4.	Verify that the plan includes special procedures such as for after-hours entry (either to the facility or to internal secured areas).			
26.5.	Verify if cameras are used for facility security. If camera surveillance is used, then verify that there is documentation on their use (e.g. how activated, how long recordings are retained, where cameras are located, etc…)			
26.6.	Verify if security guards are used for facility security. If security guards are used, then verify that their duties are documented (e.g. rounds route, frequency, check-in, etc…)			
26.7.	Verify that entries supposedly kept locked (exterior and interior) are locked.			
26.8.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Physical Safeguards – Facility Access Controls Standard – Access Control and Validation Procedures

Audit Objective:

27. Ensure that the organization has implemented procedures to control and validate all persons accessing the facility based on their role, function or visitor status. Ensure that the organization also maintains control of access to software programs for purposes of testing and revision. (Estimated Hours = 7)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
27.1.	Verify that there is policy requiring badges to be worn visibly by the workforce members.			
27.2.	Verify that policy and procedures require business and general public visitors entering the area containing PHI to wear a badge issued by the organization.			
27.3.	Verify that badges are worn consistently. (e.g. badges are visible, recognizable to the organization and to the individual wearing it if a picture Id is present).			
27.4.	Verify that there are policy and procedures for identifying visitors and/or verify that restricted areas are so marked and visitors may not enter (unless accompanied by a workforce member).			
27.5.	Verify that restricted areas have been identified and are protected from unauthorized physical access through access cards, biometrics, or other means.			
27.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Physical Safeguards – Facility Access Controls Standard – Maintenance Records

Audit Objective:

28. Ensure that the organization maintains policies and procedures to document repairs and modifications to physical components of the facility which can potentially impact security. (Estimated Hours = 12)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
28.1.	Ensure that there is a policy and procedure for documenting construction and repair work to the facility, and for reviewing work plans for any potential security impact prior to performing the work.			
28.2.	Review documentation of insurance or fire marshal appraisals of the adequacy of fire protection systems.			
28.3.	Perform a walk-through of the data center and surrounding areas and determine through observation if: a) Paper and combustible supplies are stored outside of the computer room with the exception of immediate usage requirements. b) Flammable cleaning materials kept in the computer room are maintained in small quantities. c) Areas adjoining the computer room are adequately protected from fire. d) The fire detection system has strategically located heat and smoke detection devices throughout the computer center. e) Portable fire extinguishers and fire alarms are placed strategically within the computer center with location markers visible. f) Emergency exits are clearly marked and operating. g) Emergency power shut down controls are easily accessible at exits to the data center. h) Emergency lighting is adequate throughout the computer center. i) Floor pulling devices are available, conveniently located, and well marked in the computer center. Adequate fire instructions are posted in the computer center.			
28.4.	Verify that fire extinguishers have been tested within the past year by checking the inspection date on a sample of fire extinguishers.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
28.5.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Physical Safeguards – Workstation Use Standard

Audit Objective:

29. Ensure that the organization has implemented policies and procedures that define appropriate workstation use and workstation physical attributes for all members of the workforce that access the organization's Protected Health Information (PHI). (Estimated Hours = 7)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
29.1.	Verify that policy and procedures specify what functions may be performed on user workstations.			
29.2.	Verify policy and procedures specify what functions may not be performed on workstations.			
29.3.	Verify policy and procedures specify security protections for workstation surroundings (e.g. clean desk policy).			
29.4.	Verify policy and procedures require users to log off when leaving a workstation (or invoke a password-protected screen saver when leaving for brief periods such as no more than 15 minutes). Ensure users are logging off.			
29.5.	Verify policy and procedures protecting PHI when offsite by a workforce member (e.g. on a laptop to an outside meeting).			
29.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Physical Safeguards – Workstation Security Standard

Audit Objective:

30. Ensure that the organization has implemented physical safeguards for all workstations that access Protected Health Information (PHI) in order to restrict access to authorized users. (Estimated Hours = 10)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
30.1.	Verify that an assessment of physical vulnerability of workstations in the facility has been performed.			
30.2.	Verify that the assessment resulted in either a statement that no devices are at significant risk of theft, or a statement that identified devices are at risk and will be or have been secured.			
30.3.	Determine if portable computing devices are in use for accessing or storing PHI. If portable devices are being used by the organization's workforce, verify that there is a procedure for safeguarding them. This usually means securing them with a physical lock (e.g., a cable lock or kept in a locked briefcase or file) when not in use or on one's person.			
30.4.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Physical Safeguards – Device and Media Controls Standard - Disposal

Audit Objective:

31. Ensure that the organization has implemented policies and procedures that address the final disposition of electronic Protected Health Information (PHI) stored on the organization's hardware or any other electronic media. (Estimated Hours = 8)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
31.1.	Verify that there are disposal policies and procedures.			
31.2.	Verify that the policy and procedures cover disposal of archived data at the end of its retention period.			
31.3.	Verify that the policy and procedures cover disposal of hard drives, disk packs, and other electronic storage media (e.g. compact discs, tapes, floppies,…) prior to their release.			
31.4.	Verify that the policy and procedures cover disposal of temporary files and end user files, both on workstations and on portable media.			
31.5.	Verify that end users understand the policy and procedures and are provided with a process (e.g. storage bins, utilities, etc…) for disposal of files. Procedures should apply to media stored offsite (e.g. at home) also.			
31.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Physical Safeguards – Device and Media Controls Standard – Media Re-Use

Audit Objective:

32. Ensure that the organization has implemented procedures for removal of Protected Health Information (PHI) from electronic media before the media is made available for re-use. (Estimated Hours = 2)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
32.1.	Verify that there are procedures for removing PHI prior to re-use of an electronic device or any storage media.			
32.2.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Physical Safeguards – Device and Media Controls Standard – Accountability

Audit Objective:

33. Ensure that the organization maintains documented logs of the movement its hardware and electronic media into and out of the facility, along with the individual(s) accountable for them. (Estimated Hours = 6)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
33.1.	Verify that a media log is maintained on PHI leaving the organization's facility on physical media such as tape, cartridge, or disk. The log will maintain a recording what data, who removed it, when it was moved and why.			
33.2.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Physical Safeguards – Device and Media Controls Standard – Data Backup and Storage

Audit Objective:

34. Ensure that the organization, prior to moving any equipment containing Protected Health Information (PHI), generates a retrievable, exact copy of any stored electronic PHI. (Estimated Hours = 1)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
34.1.	Verify that there is a policy or procedure statement that PHI data will be backed up before equipment maintaining the data is moved.			
34.2.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Technical Safeguards – Access Control Standard – Unique User Identification

Audit Objective:

35. Ensure that the organization has implemented a unique user identifier for purposes of tracking and granting access to the electronic information systems that maintain Protected Health Information (PHI). (Estimated Hours = 10)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
35.1.	Verify that there is a policy statement requiring unique user IDs in order to obtain access to electronic systems containing PHI.			
35.2.	Verify that access to systems accessing or transmitting PHI require a user ID.			
35.3.	Verify that there are no generic user IDs giving access to PHI. (This may entail reviewing user lists from all systems with PHI).			
35.4.	Verify that if a system requires generic system administration (sysadmin) or other similar account, it is documented. There should be procedures protecting and limiting the use of this ID.			
35.5.	Ensure that systems with PHI have adequate identifying information in the user account record to link the ID with an individual (Typically, this includes a full user name field and other identification.)			
35.6.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Technical Safeguards – Access Control Standard – Emergency Access Procedure

Audit Objective:

36. Ensure that the organization has implemented procedures for obtaining necessary electronic Protected Health Information (PHI) during an emergency event. (Estimated Hours = 3)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
36.1.	Verify that the disaster recovery plan (DRP) includes instructions for access to the organization's PHI.			
36.2.	Verify that the DRP includes all components necessary to restore the data. For example, being able to retrieve backup copies of data and software to enable the rapid restoration of systems in an emergency.			
36.3.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Technical Safeguards – Access Control Standard – Automatic Logoff

Audit Objective:

37. Ensure that the organization has implemented termination procedures that halt any electronic sessions after a predetermined time of inactivity. (Estimated Hours = 5)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
37.1.	Verify that, if an auto-logoff feature is available in systems accessing PHI, it is in use.			
37.2.	Verify that if auto-logoff is not available, it is documented and a password-protected screen saver is implemented instead.			
37.3.	Verify that the timeout period(s) is reasonable (e.g. 15 minutes). Determining whether the timeout period is reasonable is based on the degree of security risk, the physical location of the user's workstations, whether the system's vendor has an auto-logoff feature available and the complexity of the settings.			
37.4.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Technical Safeguards – Access Control Standard – Encryption and Decryption

Audit Objective:

38. Ensure that the organization has implemented encryption and decryption mechanisms on electronic systems and devices which contain Protected Health Information (PHI) stored in files and databases. This standard applies to data at rest and not data electronically transmitted. (Estimated Hours = 12)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
38.1.	Verify that an assessment has been performed by the organization to address encryption and decryption, as it pertains to PHI at rest (not in transit). If the organization has not adopted encryption and decryption mechanisms, verify that the organization has documented its own equivalent protections for PHI at rest.			
38.2.	Verify that an assessment has been performed by the organization to address encryption and decryption, as it pertains to PHI on user workstations. If the organization has not adopted encryption and decryption mechanisms, verify that the organization has documented its own equivalent protections for PHI on user workstations.			
38.3.	Verify that user files containing PHI on portables and on portable media that leave or are outside the facility, are required by policy to be encrypted.			
38.4.	Verify that affected users have encryption/decryption tools and instructions for use.			
38.5.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Technical Safeguards – Audit Controls Standard

Audit Objective:

39. Ensure that the organization has implemented hardware, software and procedural mechanisms that record and examine activity in information systems that contain or use Protected Health Information (PHI). (Estimated Hours = 11)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
39.1.	Verify that there is documentation describing what audit logs are kept.			
39.2.	Verify that the documentation for PHI-related logs identifies what events are captured on a given log, how the log is protected, and its retention period.			
39.3.	Verify that documentation identifies who is responsible for log review, how often logs are reviewed, and what criteria are users for review (to identify suspicious activity requiring investigation or other action).			
39.4.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Technical Safeguards – Integrity Standard – Mechanisms to Authenticate Electronic Protected Health Information

Audit Objective:

40. Ensure that the organization has implemented electronic mechanisms to corroborate that electronic Protected Health Information (PHI) has not been altered or destroyed. This standard applies to data at rest and not data electronically transmitted. (Estimated Hours = 8)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
40.1.	Verify whether the organization has implemented specific mechanisms to corroborate PHI integrity (at rest, not in transit). If the organization has adopted mechanisms to corroborate PHI integrity, verify that these mechanisms are documented.			
40.2.	Verify that if the organization has not adopted mechanisms to corroborate PHI integrity, that a risk assessment has been performed and it concludes that the current controls provide reasonable and appropriate alternatives, the controls and the conclusion are documented.			
40.3.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Technical Safeguards – Person or Entity Authentication Standard

Audit Objective:

41. Ensure that the organization has implemented procedures which verify that a person, entity or process seeking access to electronic Protected Health Information (PHI) has been properly identified. (Estimated Hours = 10)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
41.1.	Ensure that policy requiring access to PHI be controlled through authentication meet organizational standards.			
41.2.	Ensure that there is documentation describing the organization's authentication standards. These should include detailed password standards as well as standards for any other permitted type of authentication. (e.g. tokens, smart cards, biometrics, etc…)			
41.3.	Determine if the organizational standards require multi-factor authentication under some circumstances, and if so, that it is documented.			
41.4.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Technical Safeguards – Transmission Security Standard – Integrity Controls

Audit Objective:

42. Ensure that the organization has implemented technical and procedural security measures that ensure electronically transmitted Protected Health Information (PHI) has not been improperly modified, especially without detection, until the PHI has been properly disposed. (Estimated Hours = 15)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
42.1.	Verify that the organization's security measures to ensure electronic PHI are not improperly modified without detection while in transit, are documented.			
42.2.	Verify that the security measures are reasonable and appropriate based on risk level. (Level of risk normally varies from local network to Internet.) For example, transmission of PHI over the Internet may be required to have more stringent safeguards such as encryption and multi-factor authentication.			
42.3.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			

Department of Medical Assistance Services
Internal Audit

Audit Program

Audit or Review: 2006 DMAS and First Health Security Review

Section I: DMAS Security Environment

Security Compliance Category: Technical Safeguards – Transmission Security Standard – Encryption

Audit Objective:

43. Ensure that the organization has implemented encryption and decryption mechanisms on electronic systems and devices which transmit Protected Health Information (PHI). This standard only applies to data at being electronically transmitted and not to data at rest, stored in databases and files. (Estimated Hours = 8)

Proc. #	Audit Procedures	Page Reference	Auditor	Date Completed
43.1.	Verify that the organization has documented its position on encrypting electronic PHI in transit. For example, there may be a policy requiring encryption of all confidential data transmitted over the Internet, and the organization's data classification rules may indicate no encryption is required for other transmissions.			
43.2.	Verify that encryption tools and procedures are implemented for each mode of Internet use that might include PHI.			
43.3.	Determine if the organization's policy does not require encryption of PHI over the Internet (or not for all circumstances). If encryption is not required, the decision and rationale are to be documented. Documentation should include reference to a risk assessment.			
43.4.	Determine if the organization uses a wireless network (VPN) and encryption is used. If a wireless network is used and encryption is not, then review the documentation and rationale for the decision.			
43.5.	Follow up on any prior year recommendations. Determine whether corrective action has been completed.			